UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/856,813	08/21/2001	John Desborough Yesberg	1376-010862	3464

7590 09/13/2006

Webb Ziesenheim Logsdon
Orkin & Hanson
700 Koppers Building
436 Seventh Avenue
Pittsburgh, PA 15219-1818

EXAMINER	
COLIN, CARL G	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 09/13/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/856,813	YESBERG, JOHN DESBOROUGH	
	Examiner	Art Unit	
	Carl Colin	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 June 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12 and 14-25* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12 and 14-25* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. In response to communications filed on 6/30/2006, applicant amends claims 1, 4, 5, 7-9, 11, and 22 and adds claim 25. The following claims 1-12 and 14-25 are presented for examination.

1.1 Applicant's arguments, filed on 6/30/2006, with respect to the rejection of claims 1-12 and 14-24 have been fully considered, but they are moot in view of a new ground of rejection. The amendment to the abstract has been considered. Applicant has not overcome the 112th rejection of claims 4 and 5 and applicant's statement that the new limitation is well known is not a valid reason for adding new matter into the claims. Regarding claim 1, applicant has amended the claim to recite "wherein the digital data includes a document visually set forth obligations to which the user is to be contractually bound upon assent thereto by the user... a user operable input.. to indicate when operated by the user their assent to the obligations set forth in the document displayed on the trusted display such that document displayed cannot be repudiated". However, this limitation is not supported in the specification as explained further below in the rejection. Applicant argues that the present invention is distinct from the prior art because the prior art does not display a document. Examiner respectfully disagrees. First, Applicant's specification interchanges document with data to describe the invention. Also, Applicant's figure 3 depicts a message text as a document. Applicant's definition 7 of transaction in the response filed on 6/30/2006, admits that transaction (i.e. abstract of title, settlement of

documents, etc.) can be reasonably interpreted as document. Applicant adds that one key difference between the invention and Wang is that Wang shows a small device with a screen that displays a single line, "EFTPOS terminals also typically only shows 1-4 lines of text" as admitted by Applicant. This argument is in contradiction to Applicant's invention because figure 5 of Applicant's claimed device, display (46) shows a display that fits only 4 lines of text. In addition, Wang discloses that data pertaining to proposed transactions may then be reviewed by the user on a screen of the requesting device and further discloses that the requesting device may be a computer terminal (see column 4, lines 16-17 and 40-45). Wang discloses displayed of data pertaining to proposed transactions and the protected device has a choice to either approve or disapprove the proposed transaction; and "while the discussion has focused on transaction approvals, it should be apparent that the PEAD may be employed to conduct any kind of transaction vis-à-vis an electronic transaction system any time secured data transmission from the user to the electronic transaction system is preferred. As a further example, the PEAD may be employed to sign any computer file for authentication purposes" (see column 12, lines 45-66). Clearly the use of the PEAD is also extended to application file, which is also a document. It is noted that Applicant is arguing about a lot of features as explained above that are not claimed. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). It is further noted that Wang discloses applicant's claimed product as claimed including a communications port for receiving digital data.

> Where the only difference between a prior art product and a claimed product is printed matter that is not functionally related to the product, the content of the printed matter will not distinguish the claimed product from the prior art. *In re Ngai*, **>367 F.3d 1336, 1339, 70 USPQ2d 1862, 1864 (Fed. Cir. 2004)< (Claim at issue was a kit requiring instructions and a buffer agent. The Federal Circuit held that the claim was anticipated by a prior art reference that taught a kit that included instructions and a buffer agent, even though the content of the instructions differed.).

(See MPEP § 2112.01).

With regard to Wang and Veil's combination, Applicant's argues "if Wang had characterized the display of information as critical then it would be obvious to one of ordinary skill in the art to provide a trustworthy display. But Wang described it as optional, and so it is not obvious to make the display trusted." Wang, on the contrary, discloses using another display associated with the electronic transaction system itself if the transaction being proposed for approval is not to be displayed in the PEAD (see column 11, lines 1-5). In response to applicant's argument that "It is much better to be able to show that a system only relies for its security on the correctness of a single, small, simple component than to require that many large complex items", the fact that applicant has recognized another advantage which would flow naturally from following the suggestion of the prior art cannot be the basis for patentability when the differences would otherwise be obvious. See *Ex parte Obiaya*, 227 USPQ 58, 60 (Bd. Pat. App. & Inter. 1985). It is also noted that Wang discloses a trusted display for displaying received digital data including the document as claimed. New claim 25 also contains similar limitations. Regarding claims 6 and 25, the arguments presented by Applicant are not persuasive because these claims have nothing to do with inner and outer signatures. In fact, the inner and outer signatures described by Applicant in the response is very different from applicant's

specification (see figures 3-4 and pages 23 last paragraph to page 24) because the PKPD does not apply the inner signature (user B only) and it is signed by a user B public key. Claim 6 as originally filed was merely reciting that the storage device can hold a device key to also apply a signature. Therefore, Applicant has not overcome the rejection by amending the claims. Upon further consideration, a new ground of rejection is set forth below.

Claim Objections

2. Claims 7 and 22 are objected to as not being dependent on a preceding claim. A series of singular dependent claims is permissible in which a dependent claim refers to a preceding claim which, in turn, refers to another preceding claim.

A claim which depends from a dependent claim should not be separated by any claim which does not also depend from said dependent claim. It should be kept in mind that a dependent claim may refer to any preceding independent claim. In general, applicant's sequence will not be changed. See MPEP § 608.01(n).

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter, which the applicant regards as his invention.

Claims 1, 7-9, and 25 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Regarding claims 1 and 25 the phrase "such that document cannot be repudiated" renders the claim(s) indefinite because (page 14, paragraph 3) cited by applicant in the disclosure is not even referring to a document nor "the document cannot be repudiated;" and it is not clear what applicant means by the term above as claimed. The citation from the disclosure merely states that trusting the use of the private key and accepting that the person purported to have applied the signature actually did apply it, is a type of assurance sometimes referred as non-repudiation. Claim 25 is indefinite for reciting that the cryptographic engine is trusted to only apply user's private key to sign the received digital data while reciting a device's private key is also used to further sign the digital data. Page 23 paragraph 3 to page 24 and page 27 do not describe the limitations as claimed. Claim 25 is also rejected under 35 U.S.C. 112, second paragraph, as failing to set forth the subject matter which applicant(s) regard as their invention. Evidence that claim 25 fail(s) to correspond in scope with that which applicant(s) regard as the invention can be found in the reply filed on 6/30/2006 page 41. In that paper, applicant has stated "the DPKD's device signature provides not only the semantic indication that the inner message was created at the appropriate time but also that the signature was created using a DPKD using the trusted display regime that DPKDs apply. It is impossible for a DPKD signature to be applied to a message or document unless that document has been viewed and approved by the user on the DPKD." and this statement indicates that the invention is different from what is defined in the claim(s) because the claim only recites that a device private key can also be applied to sign the digital data. Regarding claims 1 and 25, it is also unclear what applicant means by "receiving digital data including a document visually set forth obligations... and displaying the data

including the document because the specification refers to data as document (see page 18, last paragraph through beginning of page 19).

Regarding claims 7 and 8, the new limitation renders the claims indefinite. The claim reciting the cryptographic engine verifies the received data using a key to verify... is not clear. In addition, the word "encrypt" and "sign" do not have identical meaning.

Regarding claim 9, the "said displayed received digital data" should be "said received digital data" because the displayed data was not first encrypted with a public key, and the only data displayed is the one that was signed with the private key. There is no antecedent basis for the limitation in this claim.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

4.1 Claims 1 and 25, and the intervening claims are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim contains subject matter, which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Applicant's disclosure fails to recite "wherein the

digital data includes a document visually set forth obligations to which the user is to be contractually bound upon assent thereto by the user... a user operable input.. to indicate when operated by the user their assent to the obligations set forth in the document displayed on the trusted display such that document displayed cannot be repudiated".

Claims 4, 5, and the intervening claims are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim contains subject matter, which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Applicant's disclosure fails to recite signed data is not transmitted external until said audit means records in an audit trail a record of the validation performed by said cryptographic engine and signed data is not displayed by said trusted display until said audit means records in an audit trail a record of the validation performed by said cryptographic engine. The specification, on the other hand, merely describes an audit log as a collection typically strictly chronological, of information representative of the transactions performed by the PKPD, such a log will identify typically after the fact those transactions which should not have taken place and thus unauthorized use of the signature. There is no condition being disclosed and the description does not support the claims as claimed.

Claim 11 and the intervening claims are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. Regarding claim 11, there is no disclosure of "displayed decrypted received digital data is not released external to said device unless said user operable input is operated" (see page 24, paragraph 2).

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1 and 17-20 are rejected under 35 U.S.C. 102(e) as being anticipated by US Patent 5,917,913 to **Wang**.

As per claim 1, **Wang** discloses a digital private key protection device, comprising: (see figures 3-4) a digital key storage containing a user's digital private key, for example (see column 9, lines 5-20); a cryptographic engine, for processing digital data and one or more digital keys, for example (see column 9, lines 1-6; see also figure 4); a communications port for receiving digital data from an external device that can be displayed that meets the recitation of a communications port for receiving digital data from an external device, wherein the digital data includes a document visually set forth obligations to which the user is to be contractually bound upon assent thereto by the user, and wherein the communications port is configured for transmitting data external of said digital private key protection device, for example (see column 9, lines 20-40; column 12, lines 65-67; and column 1, lines 13-35; see also figures 3-4); **Wang**

discloses a display of the electronic transaction system, display of PEAD, and display of a receiving computer terminal device that meets the recitation of trusted display for displaying said received digital data, for example (see column 10, line 65 through column 11, line 13); Wang further discloses that data pertaining to proposed transactions may then be reviewed by the user on a screen of the requesting device and further discloses that the requesting device may be a computer terminal (see column 4, lines 16-17 and 40-45); a user operable input connected to said cryptographic engine to indicate when operated by said user their assent to the obligations set forth in the document displayed on the trusted display such that document displayed cannot be repudiated, for example (see column 11, lines 14-41, column 10, lines 36-67; see also figures 3-4); wherein said cryptographic engine for processing digital data and one or more digital keys is trusted to only apply said user's digital private key to sign said received data only if said user operable input means is operated and communicate said signed data external of said digital private key protection device, for example (see column 11, lines 33-62 and column 4, lines 45-65; see also figures 3-4).

As per claim 17, **Wang** discloses the limitation of wherein said trusted display means is external to said device and controlled by said device for displaying data transmitted from said communications port in a trusted manner (see column 4, lines 40-44).

As per claim 18, **Wang** discloses wherein said user operable input means is external to said device and controlled by said device to be actuated by said user in a predetermined manner; (see column 4, lines 40-67 and column 10, line 55 through column 11, line 14).

As per claim 19, **Wang** discloses identification and authentication means actuated by said user in a predetermined manner; an audit means which audits said actuation of said user operable input means (see column 4, lines 40-67 and column 10, line 55 through column 11, line 14).

As per claim 20, **Wang** discloses an audit means, which audits said actuation of said user operable input means (see column 11, lines 50-62).

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 6-8 and 22-23, and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 5,917,913 to **Wang** in view of US Patent 6,408,388 **Fisher**.

As per claim 25, **Wang** discloses a digital private key protection device, comprising: (see figures 3-4) a digital key storage containing a user's digital private key, for example (see column 9, lines 5-20); a cryptographic engine, for processing digital data and one or more digital keys, for example (see column 9, lines 1-6; see also figure 4); a communications port for receiving digital data from an external device that can be displayed that meets the recitation of a communications port for receiving digital data from an external device, wherein the digital data includes a document to be viewed and signed so that document cannot be repudiated, and wherein the communications port is configured for transmitting data external of said digital private key protection device, for example (see column 9, lines 20-40; column 12, lines 65-67; and column 1, lines 13-35; see also figures 3-4); **Wang** discloses a display of the electronic transaction system, display of PEAD, and display of a receiving computer terminal device that meets the recitation of trusted display for displaying said received digital data including the document, for example (see column 10, line 65 through column 11, line 13); Wang further discloses that data pertaining to proposed transactions may then be reviewed by the user on a screen of the requesting device and further discloses that the requesting device may be a computer terminal (see column 4, lines 16-17 and 40-45); a user operable input connected to said cryptographic engine to indicate when operated by said user their assent to the obligations set forth in the document displayed on the trusted display such that document displayed cannot be repudiated, for example (see column 11, lines 14-41, column 10, lines 36-67; see also figures 3-4); wherein said cryptographic engine is trusted to only apply said user's digital private key to sign said received data only if said user operable input means is operated and communicate said signed data external of said digital private key protection device, for example (see column 11,

lines 33-62 and column 4, lines 45-65; see also figures 3-4). **Wang** discloses that highly sensitive may be encrypted and transmitted to the PEAD and further discloses transaction approval data may be saved along with a document to be authenticated for future reference. **Wang** also suggests that "while the discussion has focused on transaction approvals, it should be apparent that the PEAD may be employed to conduct any kind of transaction vis-à-vis an electronic transaction system any time secured data transmission from the user to the electronic transaction system is preferred. However, **Wang** is silent about using a device key for signature as to authenticating the device. **Fisher** in an analogous art discloses a method of ensuring that both the device producing the signature and the user signing the digital data can be trusted by performing multiple signatures wherein data is signed with the user's private key and is further signed with the device private key and further signing the data with the user's private key (column 6, lines 25-40 and column 8, lines 10-21). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method as combined above to store a digital private key of the device wherein digital data signed by the protection device is further signed by the private key of the protection device as taught by **Fisher**. One of ordinary skill in the art would have been lead to make such a modification because the implementation of multiple signature provides further security and trust such that both the device producing the signature and the entity can be trusted and validated as the data is signed twice with the device's key and the user's or authority's key as suggested by **Fisher** (column 6, lines 25-40). **Romney et al** in an analogous art discloses a digital private key protection device's private key wherein digital data signed by said digital private key protection device

As per claim 6, **Wang** discloses the claimed device of claim 1. However, **Wang** is silent about using a device key for signature as to authenticating the device. **Fisher** in an analogous art discloses a method of ensuring that both the device producing the signature and the user signing the digital data can be trusted by performing multiple signatures wherein data is signed with the user's private key and is further signed with the device private key and further signing the data with the user's private key (column 6, lines 25-40 and column 8, lines 10-21). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method as combined above to store a digital private key of the device wherein digital data signed by the protection device is further signed by the private key of the protection device as taught by **Fisher**. One of ordinary skill in the art would have been lead to make such a modification because the implementation of multiple signature provides further security and trust such that both the device producing the signature and the entity can be trusted and validated as the data is signed twice with the device's key and the user's or authority's key as suggested by **Fisher** (column 6, lines 25-40).

As per claims 7-8, **Veil et al** discloses use of public/private key pair for decrypting data that has been encrypted at the other end using the corresponding public or private key from the key pair (column 5, lines 48 through column 6, line 16 and discloses trusted display for verification (claim 1). **Fisher** discloses verification of signature signed by a private key using public key (column 6, line 25 through column 7, line 7). Therefore, claims 7-8 are rejected on the same rationale as the rejection of claim 25.

As per claims 22-23, the combination of **Wang and Veil et al** discloses wherein a cryptographic request is received from said external device according to a predetermined application programming interface, such that the request is performed by said digital private key protection device using the user's private or other keys as identified by the request, but excluding any private keys associated with the private key protection device with the result being transmitted to said external device or a predetermined destination included in said request or otherwise predetermined, wherein said device displays a description of said request to the user and, only if the user operates said user operable input means, does said device carry out said request (see Wang, column 11, lines 33-67).

7. **Claims 2-5, 9, 21, and 24** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 5,917,913 to **Wang** in view of US Patent US Patent 6,085,322 to **Romney et al**.

As per claim 2, **Wang** discloses the claimed device of claim 1 and discloses that the invention is not limited to any encryption scheme, for example (see column 5, lines 35-50). **Wang** discloses a digital key storage also contains a trusted public key and a plurality of user's public keys signed so as to be verifiable by the trusted public key (see column 7, lines 45-67 and column 8, lines 18-34 and lines 51-65; and figure 4); and further discloses said cryptographic engine validates signature of said user's public key with said trusted public key to determine the veracity of said user's public key (see column 7, lines 45-67 and column 8, lines 18-34 and lines 51-65); processes said received digital data using the verified predetermined user's public key (see column 7, lines 45-67 and column 8, lines 18-34 and lines 51-65); and discloses if

public/private key is used, data encrypted with a private key can be decrypted by a public key and once decrypted the data is displayed to a user for approval that meets the recitation of causes said trusted display to indicate whether said user's private key was used to sign said received data (see column 49-53 and column 12, lines 35-45). This claimed interpretation is believed by the Examiner to be broadly and reasonably interpreted because by displaying the data to the user as clear data the user can be assured that a corresponding private key was used to sign it. **Romney et al** in an analogous art discloses method and apparatus for establishing authenticity of an electronic document wherein a digital key storage also contains a trusted public key and a plurality of user's public keys signed so as to be verifiable by the trusted public key (see column 10, lines 57-61); and further discloses said cryptographic engine validates signature of said user's public key with said trusted public key to determine the veracity of said user's public key; processes said received digital data using the verified predetermined user's public key (see column 8, lines 50 through column 9, line 8); and causes said trusted display to indicate whether said user's private key was used to sign said received data (see column 9, lines 1-12). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the verification signature of Wang and provide a dialog message that indicates that the signature is good or bad as taught by **Romney et al** because the user can clearly and visually see a correct and false transaction and be alerted of a possible tampering or attack as. One of ordinary skill in the art would have been lead to make such a modification to give a user a clear and visual indication of a good digital signature as suggested by **Romney et al** (column 9, lines 1-12).

As per claim 3, **Wang** discloses that any particular cryptography algorithm may be implemented using any conventional technique (see column 5, lines 35-50), but does not explicitly disclose use of digital certificate, which is a well-known conventional technique. However, the difference is only in the nonfunctional descriptive material and does not patentably distinguish the claimed device. It would have been obvious to one of ordinary skill in the art at the time the invention was made to include any type of information in the digital data received by the device of Wang because the subjective interpretation of the information including in the digital data such as a digital certificate does not patentably distinguish the claimed device from the device of Wang.

As per claims 4-5, **Wang** discloses a audit for recording transaction and timestamp but does not explicitly disclose recording in an "audit trail" a record of the validation. **Romney et al** in an analogous art discloses a transaction log for recording transaction data concerning all transaction performed including detail of the transaction and authentication that meets the recitation of audit means records in an audit trail a record of the validation performed by said cryptographic engine and signed data is not displayed or transmitted by said trusted display until said audit means records in an audit trail a record of the validation performed by said cryptographic engine (see column 11, lines 50-55 and column 12, lines 57-60). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the device of Wang to provide a transaction log as to record pertinent transaction data in the transaction log for the purpose of verifying the data being authenticated as taught by **Romney et al** (see column 11, lines 50-55 and column 12, lines 57-60).

As per claim 9, the references as combined above disclose said received digital data contains information that predetermines which user's public key is used to encrypt said displayed received digital data that is transmitted external of said digital private key protection device to a predetermined user (see **Romney et al,** column 12, lines 29-31).

As per claim 21, the references as combined above disclose wherein said digital private key storage means is removable from said device (see **Wang,** column 7, lines 1-20 and **Romney et al,** column 7, lines 28-37).

As per claim 24, **Wang** discloses wherein said digital private key storage is adapted to allow removal of the user's digital keys from the digital private key protection device (see column 7, lines 1-20 and **Romney et al,** column 7, lines 28-37).

8. **Claims 10-12, and 14** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 5,917,913 to **Wang.**

As per claim 10, **Wang** discloses the limitation of wherein said cryptographic engine is trusted to decrypt digital data using said user's digital private key and passing decrypted digital data to said display means for display of said received digital data, for example (see column 7, lines 42-61). It is also obvious to one of ordinary skill in the art that data can be transmitted

from one PEAD to another in the transaction system, which does not depart from the spirit and scope of Wang's invention because data have to be encrypted to be received by a PEAD.

As per claim 11, **Wang** discloses displayed decrypted received digital data is not released external to said device unless said user operable input is operated (see column 8, lines 53-61; column 12, lines 7-14 and column 13, lines 1-5).

As per claim 12, **Wang** discloses wherein said communications port cannot transmit said decrypted digital data external of said digital private key protection device (see column 6, lines 43-48; column 9, lines 32-33 and column 13, lines 1-5).

As per claim 14, **Wang** discloses that any particular cryptography algorithm may be implemented using any conventional technique asymmetric and symmetric are both conventional cryptographic techniques (see column 5, lines 35-50), that meets the recitation of wherein said digital private key storage means also contains a digital shared secret symmetric key wherein said cryptographic engine is trusted to only apply said digital shared secret symmetric key to encrypt data only if said user operable input means is operated and also trusted to communicate said encrypted data external of said digital private key protection device.

9. **Claims 15-16** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 5,917,913 to **Wang** in view of **Bruce Schneier**, Applied Cryptography, 1996, John Wiley & Sons, Second Edition, Pages 43-44.

As per claims 15-16, Wang substantially teaches the claimed method of claim 1 and discloses that the invention is not limited to any encryption scheme, for example (see column 5, lines 35-50). The limitation of received data that includes instructions to determine which protocol to use to communicate or keys to use for encryption is well known in packet processing and can be also found in Schneier textbook. Neither of the references explicitly teaches validating signature of a user's public key from a plurality of public keys and decrypts data using the verified public key. **Schneier** in an analogous art teaches a key certification authority wherein the users' public keys are signed with a trusted private key to prevent attack against public key, for example (see pages 43, 62-64); and further discloses validating signature of said user's public key with said trusted public key to determine the veracity of said user's public key and then decrypts said received data using said verified predetermined user's public key, for example (see pages 43, 62-64). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method as combined above to store user's public keys and have the public keys signed by a trusted private key using public/private key pairs as taught by **Schneier**. This modification would have been obvious because one skilled in the art would have been motivated by the suggestions provided by **Schneier** to have a card that can be used by more than one user and prevent attack against public key and prevents users from repudiation as it proves proof of user's participation.

Conclusion

10. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

10.1 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

cc

Carl Colin
Patent Examiner
September 11, 2006

NASSER MOAZZAMI
PRIMARY EXAMINER

9,11,06